

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-112491

(43) 公開日 平成11年(1999) 4月23日

(51) Int.Cl.*	識別記号	F I
H 0 4 L 9/14		H 0 4 L 9/00
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00

審査請求 未請求 請求項の数 4 O L (全 8 頁)

(21) 出願番号 特願平9-272793

(22) 出願日 平成9年(1997)10月6日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 加藤 岳久

東京都府中市東芝町1番地 株式会社東芝

府中工場内

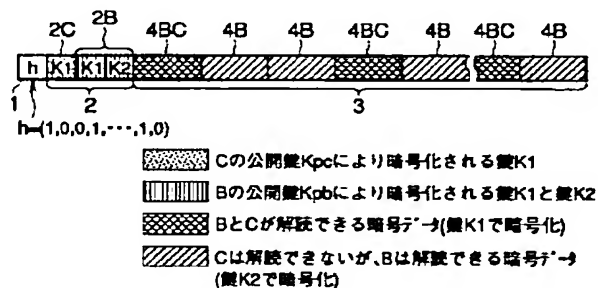
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 発信情報監視方法及び端末装置

(57) 【要約】

【課題】 本発明は、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライバシー保護も実現する。

【解決手段】 データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、情報3を複数のブロックに分割する分割ステップST4と、複数のブロックのうち一部のブロック4BCを、発信情報を監視する者C及び受信者B双方に復号可能に暗号化する第1の暗号化ステップST4と、複数のブロックのうち一部のブロックを除く他のブロック4Bを、受信者のみに復号可能に暗号化する第2の暗号化ステップST4とを有する発信情報監視方法。



【特許請求の範囲】

【請求項 1】 送信データを含む伝送フレームを作成するフレーム作成部と、

前記フレームを複数のブロックに分割するフレーム分割処理部と、

前記複数のブロックのうちいくつかのブロックを第 1 の変換コードに基づいてコード化し、更に残りのブロックを第 2 の変換コードに基づいてコード化する変換処理部とを有することを特徴とする端末装置。

【請求項 2】 データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、前記情報を複数のブロックに分割する分割ステップと、前記複数のブロックのうち一部のブロックを、発信情報を監視する者及び受信者双方に復号可能に暗号化する第 1 の暗号化ステップと、前記複数のブロックのうちの前記一部のブロックを除く他のブロックを、前記受信者のみに復号可能に暗号化する第 2 の暗号化ステップとを有することを特徴とした発信情報監視方法。

【請求項 3】 前記複数のブロックのうち、何れのブロックが第 1 の暗号化ステップで暗号化されるかを示す識別情報を発信情報に付加するステップを有することを特徴とした請求項 2 記載の発信情報監視方法。

【請求項 4】 前記第 1 の暗号化ステップ及び前記第 2 の暗号化ステップにおいては、前記複数のブロックのうち、それぞれどのブロックを暗号化するかを情報発信者に知られることなく、当該暗号化を行うことを特徴とした請求項 2 又は 3 記載の発信情報監視方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は発信情報監視方法及び端末装置、特にネットワークを用いてデータや通信文を暗号化して通信し合う場合に、その発信情報の監視に適した発信情報監視方法及び端末装置に関するものである。

【0002】

【従来の技術】 近年のネットワーク技術の発達、ネットワーク通信の活発化に伴い、公衆回線等の通信網上を流れる情報を悪意者等からいかに守るかということが極めて重要になってきている。

【0003】 このため、通信を行う際にそのデータや通信文を暗号化することが行われている。例えば社内 LAN から公衆回線を通じて社外にデータや電子メール等を発信する場合、受信者のみがその情報を復号できるように発信者が発信情報に暗号化をかけるシステムの導入も検討されている。

【0004】

【発明が解決しようとする課題】 しかしながら、ネットワークを用いてデータや通信文を暗号化して通信を行う場合、その暗号化された情報が、例えば企業秘密のよう

な企業外へ漏洩してはいけない情報が否かを監査することは従来の技術では困難である。

【0005】 一方、仮に社内 LAN から発信されるすべての情報についてその内容を検査するシステムを構築したのでは、企業秘密情報のみならず、個人的な電子メール等の情報まですべて検査されることになる。しかし、これはプライバシー保護の観点から妥当ではなく、また過度な情報監視は企業活動を停滞させてしまう可能性もある。

【0006】 本発明は、このような実情を考慮してなされたもので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライバシー保護も実現する発信情報監視方法及び端末装置を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記課題を解決するために、請求項 1 に対応する発明は、送信データを含む伝送フレームを作成するフレーム作成部と、フレームを複数のブロックに分割するフレーム分割処理部と、複数のブロックのうちいくつかのブロックを第 1 の変換コードに基づいてコード化し、更に残りのブロックを第 2 の変換コードに基づいてコード化する変換処理部とを有する端末装置である。

【0008】 本発明は、このような手段を設けたので、送信データを含む伝送フレームが複数のブロックに分割される。そして、この複数のブロックのうちいくつかのブロックが第 1 の変換コードに基づいてコード化され、更に残りのブロックが第 2 の変換コードに基づいてコード化される。このとき例えば、第 1、第 2 の変換コードによりブロックを暗号化することも可能である。

【0009】 また、請求項 2 に対応する発明は、データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、情報を複数のブロックに分割する分割ステップと、複数のブロックのうち一部のブロックを、発信情報を監視する者及び受信者双方に復号可能に暗号化する第 1 の暗号化ステップと、複数のブロックのうち一部のブロックを除く他のブロックを、受信者のみに復号可能に暗号化する第 2 の暗号化ステップとを有する発信情報監視方法である。

【0010】 本発明は、このような手段を設けたので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライバシー保護も実現させることができる。つまり発信情報をブロック化し、このブロックを受信者のみに解読できるブロックと、受信者及び監視者双方に解読できるブロックとにわけることによって、秘密漏洩の有無を確認しつつ全発信情報を見ないことでプライバシー保護をも図るものである。これは全発信情報を確認しなくても秘密漏洩の有無程度はチェックできることに着目したものである。

【0011】 さらに、請求項 3 に対応する発明は、請求

項 2 に対応する発明において、複数のブロックのうち、何れのブロックが第 1 の暗号化ステップで暗号化されるかを示す識別情報を発信情報に付加するステップを有する発信情報監視方法である。

【0012】本発明は、このような手段を設けたので、請求項 2 に係る発明と同様な作用効果が得られる他、受信者は、この発信情報に付加された識別情報により、効率的に上記一部のブロックを監査し、また受信者は効率的に全ブロックを解読することができる。

【0013】さらにまた、請求項 4 に対応する発明は、請求項 2 又は 3 に対応する発明において、第 1 の暗号化ステップ及び第 2 の暗号化ステップにおいては、複数のブロックのうち、それぞれどのブロックを暗号化するかを情報発信者に知られることなく、当該暗号化を行う発信情報監視方法である。

【0014】本発明は、このような手段を設けたので、請求項 2 又は 3 に係る発明と同様な作用効果が得られる他、第 1 及び第 2 の暗号化ステップにおいては、複数のブロックのうち、それぞれどのブロックが暗号化されるかが情報発信者に対して秘密にされる。したがって、発信者は上記一部のブロックを特定できず、秘密情報を上記他のブロックに該当する部分に秘匿することができないため、秘密情報の発信監査をより一層効果的に行うことができる。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第 1 の実施の形態）図 1 は本発明の第 1 の実施の形態に係る発信情報監視方法が適用される場面を想定した図である。

【0016】同図において、A は送信者で B は受信者である。C は A が発信する通信内容を監視する監査人である。このような場面は、例えば A はある会社の社員であり、C は A の会社の社長とする。B は A と C の会社以外の人間であると仮定する。

【0017】本実施形態では、A と B は RSA 暗号方式等の公開鍵暗号を用いて暗号通信を行うものとする。ここでは、同図に示すように、A は公開鍵 K_{pa} と秘密鍵 K_{sa} を有しており、同様に B は公開鍵 K_{pb} と秘密鍵 K_{sb} 、C は公開鍵 K_{pc} と秘密鍵 K_{sc} を有している。なお、RSA 暗号（公開鍵暗号）を用いた暗号通信の方法については、「現代暗号理論」池野信一、小山謙二 共著、電子情報通信学会編、p. 105-123 や「暗号理論入門」岡本栄司 著、共立出版株式会社、p. 88-99 等にも記載されている。

【0018】このような場合に、A が B に向けて発信した個人的な秘密情報を全て第三者である監査人 C に知られることなく、A が B に向けて発信した内容が会社の秘密情報ではないかについて、すなわち A が会社の秘密情報を漏洩していないかについて監査人 C が調べる方法を

説明する。

【0019】図 2 は本実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図である。同図に示す A が送信するデータ並び、つまり送信パケット（例えばメール）においては、データ本体 3 の先頭に、ヘッダ情報部 1 と鍵情報部 2 とが順次付加されている。

【0020】このデータ本体 3 は、等しい大きさのブロック 4 B、4 BC（以下、単にブロック 4 ともいう）に分割されている。このブロック 4 の大きさは、例えば暗号化を行うためのブロックの大きさである。

【0021】このブロック 4 のうち、一部（全部を含む）のブロック 4 BC のみ監査人 C により復号できるようになっている。監査人 C は自己の復号可能なブロック 4 BC を決定し、このヘッダ情報は A には知らせない。

【0022】図 2 においてヘッダ情報部 1 には、どのブロックが監査人 C が復号できるのかがヘッダ情報 h として格納されている。なお、同図に例示されるヘッダ情報 h において、h = 1 の部分は暗号ブロック 4 BC に対応し、h = 0 の部分が暗号ブロック 4 B に対応している。

【0023】このように、監査人 C が復号できるブロック 4 BC が A により特定できないようにすることで、発信者 A は、漏洩してはいけない秘密情報を監査人 C に発見できないように操作することが不可能となる。

【0024】図 2 の例では、ブロック 4 BC が監査人 C と受信者 B が復号できる、すなわち鍵 K 1 で暗号化された暗号ブロックであり、ブロック 4 B が受信者 B のみが復号できる、すなわち鍵 K 2 で暗号化された暗号ブロックである。

【0025】各ブロック 4 について、ブロック 4 BC は B、C が復号でき、ブロック 4 B は B のみが復号できるのは、ブロック 4 BC を暗号化する鍵 K 1 と、ブロック B を暗号化する鍵 K 2 とが暗号化されて鍵情報部 2 に格納されているからである。

【0026】鍵情報部 2 は、B 用鍵部 2 B と C 用鍵部 2 C からなっている。B 用鍵部 2 B は、B の公開鍵 K_{pb} により暗号化された鍵 K 1 及び鍵 K 2 が格納されており、B の秘密鍵 K_{sb} のみにより鍵 K 1 及び鍵 K 2 の取出しが可能である。一方、C 用鍵部 2 C は、C の公開鍵 K_{pc} により暗号化された鍵 K 1 のみが格納されており、C の秘密鍵 K_{sc} のみにより鍵 K 1 の取出しが可能である。

【0027】したがって、この送信パケットから監査人 C は、鍵 K 1 のみを得ることができ、ブロック 4 BC のみを監査することができる。一方、受信者 B は、この送信パケットから鍵 K 1 及び鍵 K 2 を得ることができ、ブロック 4 BC 及びブロック 4 B、すなわちデータ本体 3 のすべてを読むことができる。

【0028】次に、この発信情報監視方法を実現するシステムの一例について具体的に説明する。図 3 は本実施

形態に係る発信情報監視方法を適用するネットワークシステムの構成例を示すブロック図である。

【0029】このネットワークシステムは、通信手段としての公衆回線網11を介してC社LAN12とB用システム13が接続されて構成されている。C社LAN12においては、データ伝送路21に、社員Aの使用するA用端末22の他、A用端末22と同様な構成の他の社員用の端末23が複数接続され、さらに、C用端末24、メールサーバ25及びその他図示しないホスト計算機等が接続されている。

【0030】メールサーバ25は、ネットワーク接続装置を兼ねるものであり、公衆回線網11を介してメールを授受すると共に、C社LAN12のデータ伝送路21上のメールを取り込み、所定の規則に従って公衆回線網11に送出するようになっている。

【0031】A用端末22や端末23は、文書やデータ作成等の基本的な計算機機能を実行できる他、メーラ26が設けられ、作成したデータや文書をメールサーバ25を介して公衆回線網11に送出できるようになっている。

【0032】メーラ26は、ヘッダ付加部27及び暗号化部28を備え、暗号化された上記送信パケットにあて先等の必要な情報を付加し、メールとしてデータ伝送路21上に送出する。

【0033】ヘッダ付加部27は、メール送信の際に、C用端末24からヘッダ情報hを受け取るとともに、そのヘッダ情報hを暗号化部28に通知し、暗号化部28により暗号化されたデータ本体3及び鍵情報部2に、ヘッダ情報部1を付加する。なお、ヘッダ付加部27は、発信者Aの操作によってはヘッダ情報hを読み出すことができないように構成されており、メール発信前に発信者Aがヘッダ情報hの内容を知ることはない。

【0034】暗号化部28は、ヘッダ付加部27から受けたヘッダ情報hに基づき、データ本体3をブロックに分割し暗号化すると共に、そのデータ本体3を暗号化するのに用いた鍵をさらに暗号化して鍵情報部2に格納する。

【0035】一方、C用端末24は、監視ブロック設定部29を備えC社LAN12から発信されるデータ（メール）の監査するブロックを設定可能になっている他、メールサーバ25に対してC社LAN12から発信されるすべてのメールについて監査できるようになっている。さらに、メールサーバ25がどのような条件でメールを発信するかを設定できるようになっている。

【0036】監視ブロック設定部29は、Cが監査できるブロック4BCを決定する情報であるヘッダ情報を生成する。監視ブロック設定部29の機能である監査人Cが復号できるブロック数nの決定方法としては、例えばAが送信する情報の総ブロック数mを上限とし、ランダムな正の整数 $0 < n < m$ を生成する方法がある。また、

この下限と上限は監査人Cが任意に決定するようにしてもよい。

【0037】また、監視ブロック設定部29が監査人Cが復号できるブロック4BCをどのような配置とするかは、例えばAがBに対して通信を行う日付や時間情報を元に、ランダム変数を決定することで行う。

【0038】なお、このヘッダ情報hは秘密情報であり、監査人C以外は知ることができないよう各部29、26、27、28等は構成されている。また、上記したメールサーバ25に設定する条件というのは、例えば監査済みのメールのみを発信可能とするとか、また例えばメールサーバ25が取り込んでから所定時間を経過したメールのみを発信するようにするとか、さらに監査人Cが指定した所定の発信者のメールのみを監査終了まで発信しないようにする等が考えられる。

【0039】次に、以上のように構成された本発明の実施の形態に係る発信情報監視方法を適用したシステムの動作について説明する。図4は本実施形態の発信情報監視方法を適用したシステムの動作を示す流れ図である。

【0040】まず、監査人によって、ヘッダ情報の設定がなされる（ST1）。この情報設定は、C社LAN12に接続された端末22、23すべてについて一括で行ってもよく、また、個々に行ってもよい。ここでは監視ブロック設定部29により、予めヘッダ情報が決定されている。

【0041】次に、発信者Aにより送信されるデータが作成され、さらに暗号化通信に必要なBの公開鍵Kpb及びCの公開鍵Kpcが用意される（ST2）。なお、公開鍵Kpb、Kpcは、暗号化部28に事前に登録されている。

【0042】次に、発信者Aによりメーラ26に対してデータの送信依頼が行われる（ST3）。これにより、メーラ26により監視ブロック設定部29からヘッダ情報が要求され、取得されたヘッダ情報に基づき、発信データのブロック化が行われる。さらに、監査人Cの復号できるブロック4BCが鍵K1、監査人Cが復号できず受信者Bのみが復号できるブロック4Bが鍵K2により暗号化される（ST4）。なお、本動作例ではステップST1でヘッダ情報は予め決定されているとしたが、ヘッダ情報決定方法としては、上述したように例えば発信者Aが受信者Bに対して通信を行う日付や時間情報を元に、ランダムにかつ個々にヘッダ情報を決定してもよい。このような決定方法を用いる場合には、上記ステップST1は、本ステップST4にてメーラ26がヘッダ情報を監視ブロック設定部29に要求したときに行われる。

【0043】次に、鍵K1が監査人Cの公開鍵Kpcで暗号化され、また鍵K1及び鍵K2が受信者Bの公開鍵Kpbで暗号化され（ST5）、暗号化されたデータ本体3に鍵情報部2、ヘッダ情報1が付加され、メール用

の送信パケットが完成される。

【0044】こうして完成されたパケットがメーラ26によりデータ伝送路21に送出され、メールサーバ25により、このパケットが取得される(ST7)。このメールサーバ25に格納されたパケット(B宛メール)は監査人Cにより監査される。すなわち監査人Cは、自分の公開鍵K_{pc}で暗号化された鍵K1を自分の秘密鍵K_{sc}で復号して、鍵K1を取り出す。なお鍵K2は取り出すことができない。監査人Cは、ヘッダ情報hに基づき、取り出した鍵K1により解読可能なブロック4BCのみを復号し内容を確認する(ST8)。

【0045】監査後、メールサーバ25によりB宛のメール(送信パケット)が公衆回線に送出され、B用システム13で受信される(ST9)。メールを受け取った受信者Bは自分の秘密鍵K_{sb}を用いて、自分の公開鍵K_{pb}で暗号化された鍵K1と鍵K2を復号し取り出す。そしてヘッダ情報hに基づいて、鍵K1で暗号化されたブロック4BCを復号し、かつ鍵K2で暗号化されたブロック4Bを復号する。これによりメール内の全情報を解読することができる。

【0046】上述したように、本発明の実施の形態に係る発信情報監視方法は、発信者Aが発信するデータを複数のブロックに分割すると共に、各ブロックを監査人Cと受信者Bが復号可能に暗号化されたブロック4CBと、受信者Bのみが復号可能に暗号化されたブロック4Bの何れかとして送信パケットを構成するようにしたので、発信情報が例えば企業秘密のような秘密情報でないかを監査人が監査することができる。これにより企業秘密等の秘密情報の漏洩を防止することができるとともに、発信者は通信内容を全て監査人に開示することなく相手(受信者)に暗号通信を行うことができる。なお、受信者は通信内容を全て復号できる。

【0047】また、復号するための鍵を監査人のみが復号できる鍵と、相手(受信者)が復号できる鍵とに分けて送信することにより、第三者に通信を盗聴することを防止することができる。

(発明の第2の実施の形態)本実施形態は、第1の実施形態とは異なる形式の送信パケットを用いることで機密情報漏洩を監視する方法について説明する。

【0048】図5は本発明の第2の実施の形態に係る発信情報監視方法が適用される場面を想定した図であり、図1と同一部分には同一符号を付してその説明を省略する。同図に示す場合、発信者Aと受信者Bはお互いが共有する秘密鍵である共有鍵K_{sab}を持っている。監査人Cはこの共有鍵K_{sab}がどのようなものであるかを知らない。

【0049】図6は本実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図であり、図2と同一部分には同一符号を付してその説明を省略する。この送信パケットは、ヘッダ情報部1と鍵情報部2

とデータ本体3とから構成されている。また、本実施形態ではB用鍵部2B'に共有鍵K_{sab}で暗号化された鍵K1が格納され、Bのみが解読できるブロック4B'が共有鍵K_{sab}で暗号化されている点を除けば第1の実施形態と同様に構成されている。なお、図6に例示するヘッダ情報hとブロック4BC、4B'の対応関係は第1の実施形態と同様である。

【0050】また、この発信情報監視方法を適用したシステムも図3に示す第1の実施形態と同様に構成されている。ただし、暗号化に共有鍵K_{sab}が用いられ、かつ、図6のパケットが作成されるように暗号化部28の構成が変更される点が第1実施形態と異なっている。

【0051】次に、本実施形態の発信情報監視方法における処理の流れについて説明する。システム全体の動作は図4に示す処理流れと同様である。パケット構成及び使用する鍵の相違による第1実施形態との処理の違いについて説明する。

【0052】本実施形態では、図4のステップST4において監査人Cが復号できるブロック4BCは鍵K1で暗号化される。また、ステップST5にて鍵K1は監査人Cの公開鍵K_{pc}で暗号化され、C用鍵部2Cに格納される。

【0053】一方図4のステップST4において、監査人Cが復号できずBのみが復号できるブロック4B'は、共有鍵K_{sab}で暗号化される。また、ステップST5にて鍵K1が共有鍵K_{sab}で暗号化され、B用鍵部2B'に格納される。なお、鍵K1は第1実施形態と同様にBの公開鍵K_{pb}にて暗号化してもよい。

【0054】またブロックが監査人Cが復号できるブロック4BC、すなわち鍵K1で暗号化したブロック4CBか否かを示す情報hは、第1実施形態と同様にヘッダ情報部1に納められる。

【0055】こうしてメーラ26により作成されたパケットはメールサーバ25に送出される。監査人Cはメールサーバ25にアクセスし、自分の公開鍵K_{pc}で暗号化された鍵K1を自分の秘密鍵K_{sc}で復号して、鍵K1を取り出す。なお、共有鍵K_{sab}は知らない。このため監査人Cは、ヘッダ情報hに基づいて、鍵K1で暗号化されたブロックのみ復号する。

【0056】一方、送信パケットを受信した受信者Bは、送信者Aとの共有鍵K_{sab}を用いて、共有鍵K_{sab}で暗号化された鍵K1を復号し取り出す。そしてヘッダ情報hに基づいて、鍵K1で暗号化されたブロックを復号し、かつ共有鍵K_{sab}で暗号化されたブロックを復号する。

【0057】上述したように、本発明の実施の形態に係る発信情報監視方法は、第1の実施形態と同様な手段を設けた他、ブロック4Bを共有鍵K_{sab}で暗号化するようにしたので、第1の実施形態と同様な効果を得ることができる。また、本実施形態の場合には、受信者Bの

共有鍵 $K_{s a b}$ を用いることで、受信者 B が公開鍵方式の公開鍵及び秘密鍵を有する必要をなくすることができる。

【0058】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。例えば第 1 の実施形態では、A、B、C が公開鍵及び秘密鍵を有する場合を説明し、第 2 の実施形態では、A と B が共有鍵 $K_{s a b}$ を有する場合で説明したが、各人が所有する鍵及び対応する暗号化についてはこのような場合に限られるものではない。つまり、種々の暗号化方式や各人の種々な鍵所有ケースに適宜対応して本発明を適用できるものである。

【0059】また例えば上記各実施形態では、ヘッダ情報 h をまとめてパケットの先頭に付加するようにしたが、ヘッダ情報 h の付加方法は、このような方法に限られるものではない。

【0060】図 7 はヘッダ情報 h 夫々を対応するブロックの先頭に別々に設けた場合における送信情報のデータ並びの一例を示す図である。このようにヘッダ情報 h は、図 2 や図 6 に示すようにヘッダ情報部 1 としてまとめて設けてもよいし、図 7 に示すように各暗号ブロック 4 の前に分散されたヘッダ情報部 1' として設けてもよい。

【0061】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウェア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD 等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。

【0062】

【発明の効果】以上詳記したように本発明によれば、発信者により暗号化された情報を監査人により部分的に復号できるようにしたので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライベート保護も実現する発信情報監視方法及び端末装置を提供することができる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施の形態に係る発信情報監視方法が適用される場面を想定した図。

【図 2】同実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図。

【図 3】同実施形態に係る発信情報監視方法を適用するネットワークシステムの構成例を示すブロック図。

【図 4】同実施形態の発信情報監視方法を適用したシステムの動作を示す流れ図。

【図 5】本発明の第 2 の実施の形態に係る発信情報監視方法が適用される場面を想定した図。

【図 6】同実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図。

【図 7】ヘッダ情報 h 夫々を対応するブロックの先頭に別々に設けた場合における送信情報のデータ並びの一例を示す図。

【符号の説明】

1 …ヘッダ情報部

2 …鍵情報部

2 B … B 用鍵部

2 C … C 用鍵部

3 …データ本体

4 B … B のみが復号できるブロック

4 B C … B 及び C が復号できるブロック

1 1 …公衆回線網

1 2 …C 社 LAN

1 3 …B 用システム

2 1 …データ伝送路

2 2 …A 用端末

2 3 …A 以外の社員が使用する端末

2 4 …C 用端末

2 5 …メールサーバ

2 6 …メーラ

2 7 …ヘッダ付加部

2 8 …暗号化部

2 9 …監視ブロック設定部

A …発信者

B …受信者

C …監査人

K 1 …鍵

K 2 …鍵

K p a …A の公開鍵

K p b …B の公開鍵

K p c …C の公開鍵

K s a …A の秘密鍵

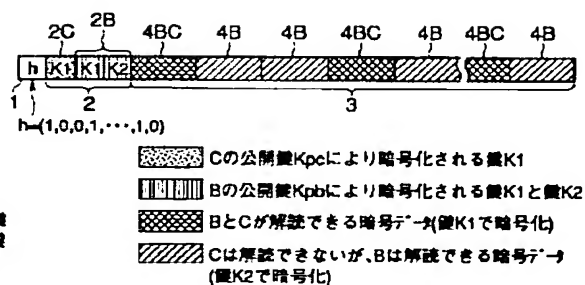
K s a b …A、B の共有鍵

K s b …B の秘密鍵

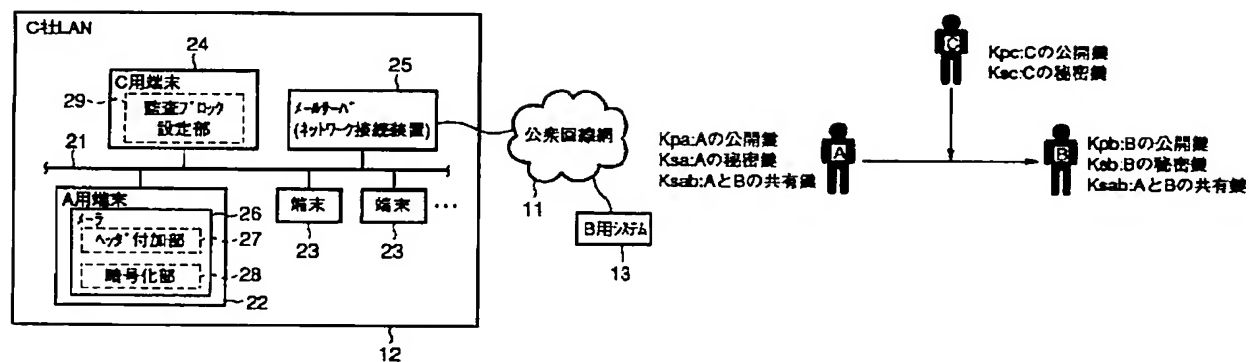
K s c …C の秘密鍵

h …ヘッダ情報

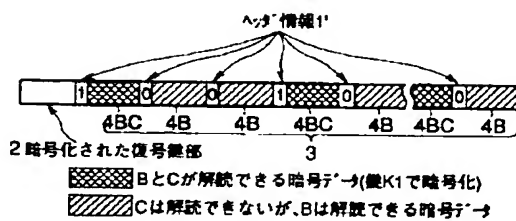
【圖 2】



【圖 5】



【図 7】



【図 4】

